

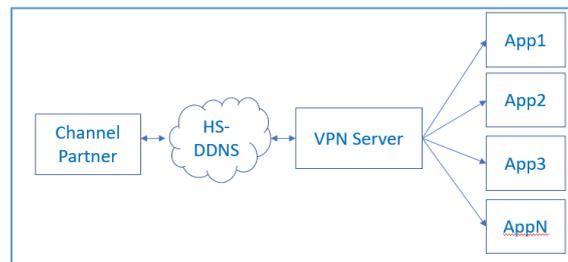
Hyperscalers R&D lab VPN access

HyperScalers R&D laboratory helps customers find a suitable cloud computing **“Appliance as a Solution”**; by documenting design and deployment guidelines, proven configurations; with bill of materials, coordinated support, and expert services. The advantages a customer gets by this approach are; he gets a designed, prebuilt, tested and calibrated cloud based solution before actual investments.

This document describes methods by which customers can login to any appliance executing in the lab. The methods provide an VPN like access to the customers; via which they can execute their workloads on these appliances. There are two ways a customer (or channel partner) can login to appliances.

1. Using remote desktop connection

The HS lab has a dedicated Windows Server box to facilitate any channel partner who wants to access the appliances. The box can internally connect to all appliances; and its exposed to the external network using a dedicated DDNS port. This setup needs to be integrated with the hyperscalers website; so that there is way to connect for any valid channel partner.



Steps 1:

The channel partner logs in the hyperscalers.com website and goes to Solutions -> The Lab tab.



The channel partners would have a valid credentials to login into the website.

Steps 2:

“The lab” tab would have list of all appliances available in the lab; which can be verified by the channel partner. Once he clicks any of the tabs; there would be an email sent to the registered mail-id; where all the login and access details would be there for the users.

Steps 3:

The channel partner will get the link of Hyperscalers DDNS which can be used to connect to the remote desktop of VPN server. On the remote desktop all appliances are made accessible, and administrator would maintain the login credentials and ways to access individual appliance.

Following table gives details of appliances accessible in the lab:

DDNS Remote Desktop Access	hyperscalers.asuscomm.com:200
MoxRox	Appliance IP: https://192.168.59.74:8006
OpenQRM	Appliance IP: http://192.168.1.76/openqrm

HyperScalers is an Australian registered company.

ABN - 83 600 687 223

ACN - 600 687 223

VmWare ESxi	Appliance IP: https://192.168.1.204
Nexenta	Appliance IP: https://192.168.18.62:8457
Redhat Openstack	Appliance IP: http://192.168.18.125/dashboard
Redhat Openshift	BMC IP: http://192.168.17.107/index.html
Redhat Gluster	SSH IP: 192.168.18.230

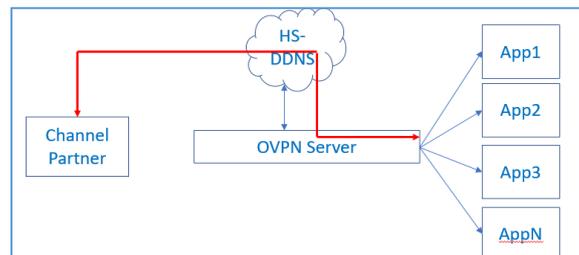
The login credential of each appliance and desktop should be maintained by the administrator.

2. Using HS router VPN

On the customer requirements, the R&D lab can also share a dedicated VPN access tunnel for specific appliance. That would be used only if the customer needs to execute their test loads or scripts on the appliance. The router connected to the lab network would provision a OpenVPN access for specific customers.

3. Dedicated VPN server for R&D lab

The R&D lab is working on designing a dedicated VPN server for all the appliances; that should open a tunnel specific to the appliance with dedicated login credentials for each user.



The design provides a management window in the OVPN server; which would enable the administrator to create a ovpn login for channel partner; and associate the IP address of appliance which is needed by the partner. This would be based on open source solutions; and it's a work in progress.